Software & Supply Chain Assurance:

Increasing Government Accountability for Cyber Risk Management by Addressing Enterprise Security Needs through Contract Management for ICT Services

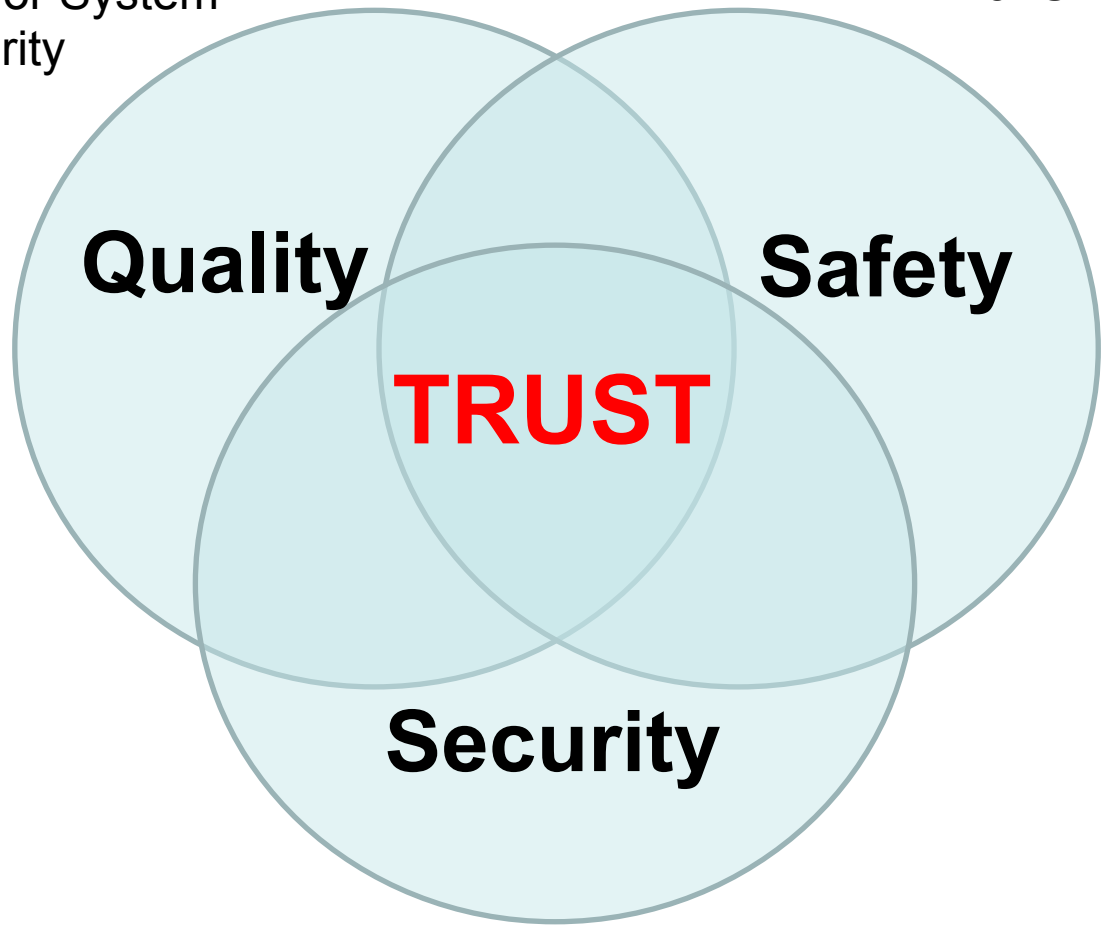
Homeland Security

Joe Jarzombek, PMP, CSSLP
Director for Software & Supply Chain Assurance
Stakeholder Engagement & Cyber Infrastructure Resilience
Cyber Security & Communications

Assurance relative to Trust

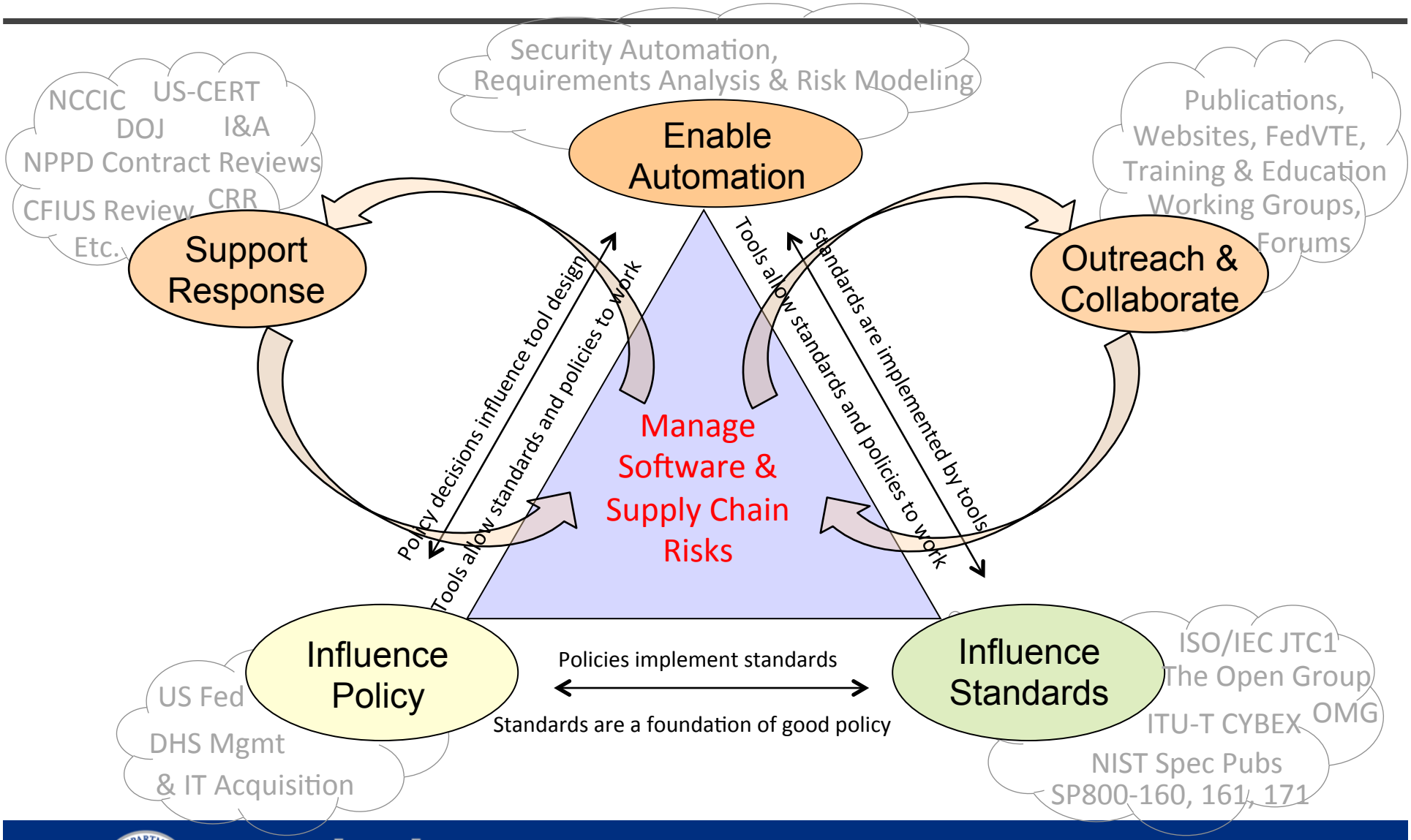
Managing Effects of Unintentional Defects in Component or System Integrity

Managing Consequences of Unintentional Defects



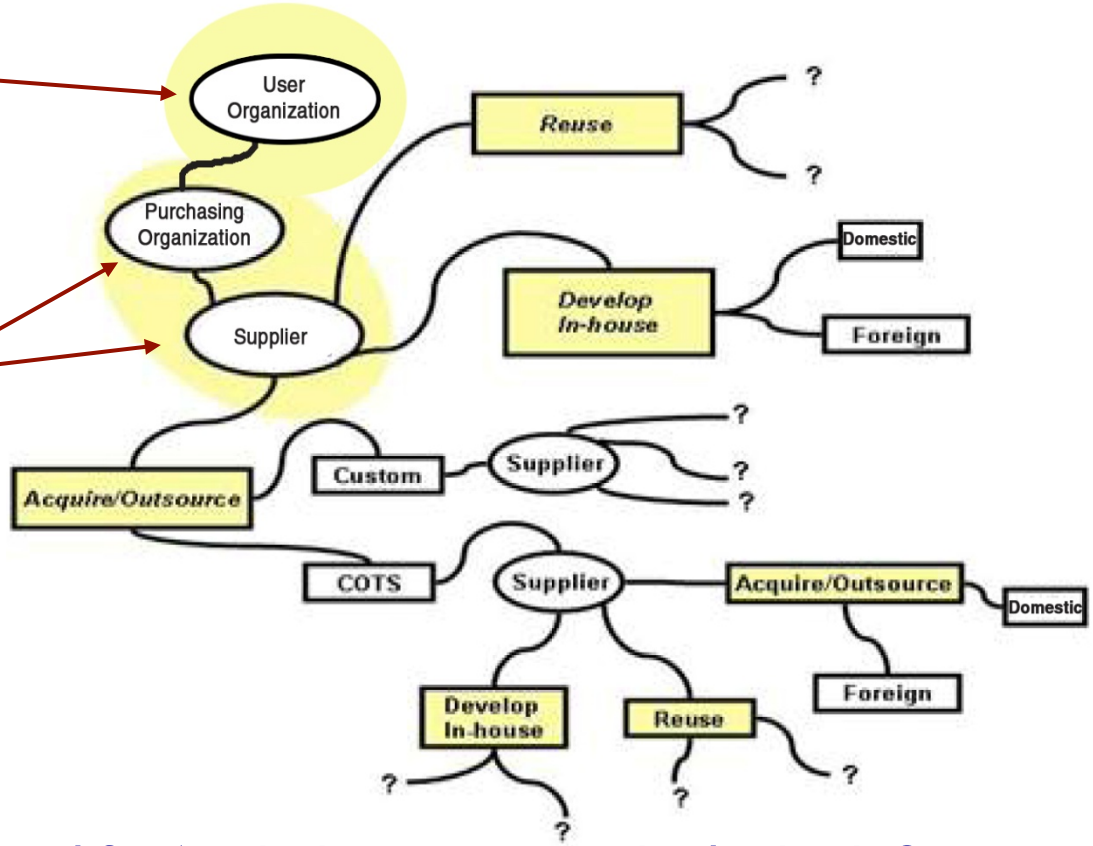
Managing Consequences of Attempted/Intentional Actions Targeting Exploitable Constructs, Processes & Behaviors

DHS Software & Supply Chain Assurance Strategy



Risk Management (Enterprise ⟷ Project):
Shared Processes & Practices ⟷ Different Focuses

- Enterprise-Level:
  - Regulatory compliance
  - Changing threat environment
  - Business Case
- Program/Project-Level:
  - Cost
  - Schedule
  - Performance



Who makes risk decisions?
Who determines 'fitness for use' for 'technically acceptable' criteria?
Who "owns" residual risk from non-secure products and services?

* "Tainted" products are those that are corrupted with malware, or exploitable weaknesses & vulnerabilities that put users at risk

Homeland Security

We Have a Problem

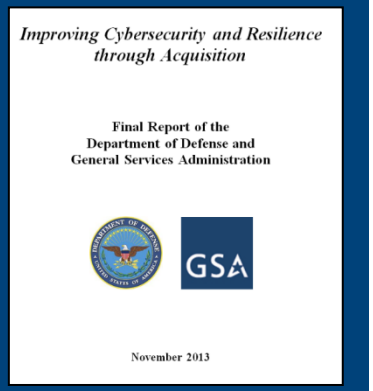
- When the government purchases products or services with inadequate in-built “cybersecurity,” the risks created persist throughout the lifespan of the item purchased. The lasting effect of inadequate cybersecurity in acquired items is part of what makes acquisition reform so important to achieving cybersecurity and resiliency.
- Currently, government and contractors use varied and nonstandard practices, which make it difficult to consistently manage and measure acquisition cyber risks across different organizations.
- Meanwhile, due to the growing sophistication and complexity of ICT and the global ICT supply chains, federal agency information systems are increasingly at risk of compromise, and agencies need guidance to help manage ICT supply chain risks

Executive Order 13636

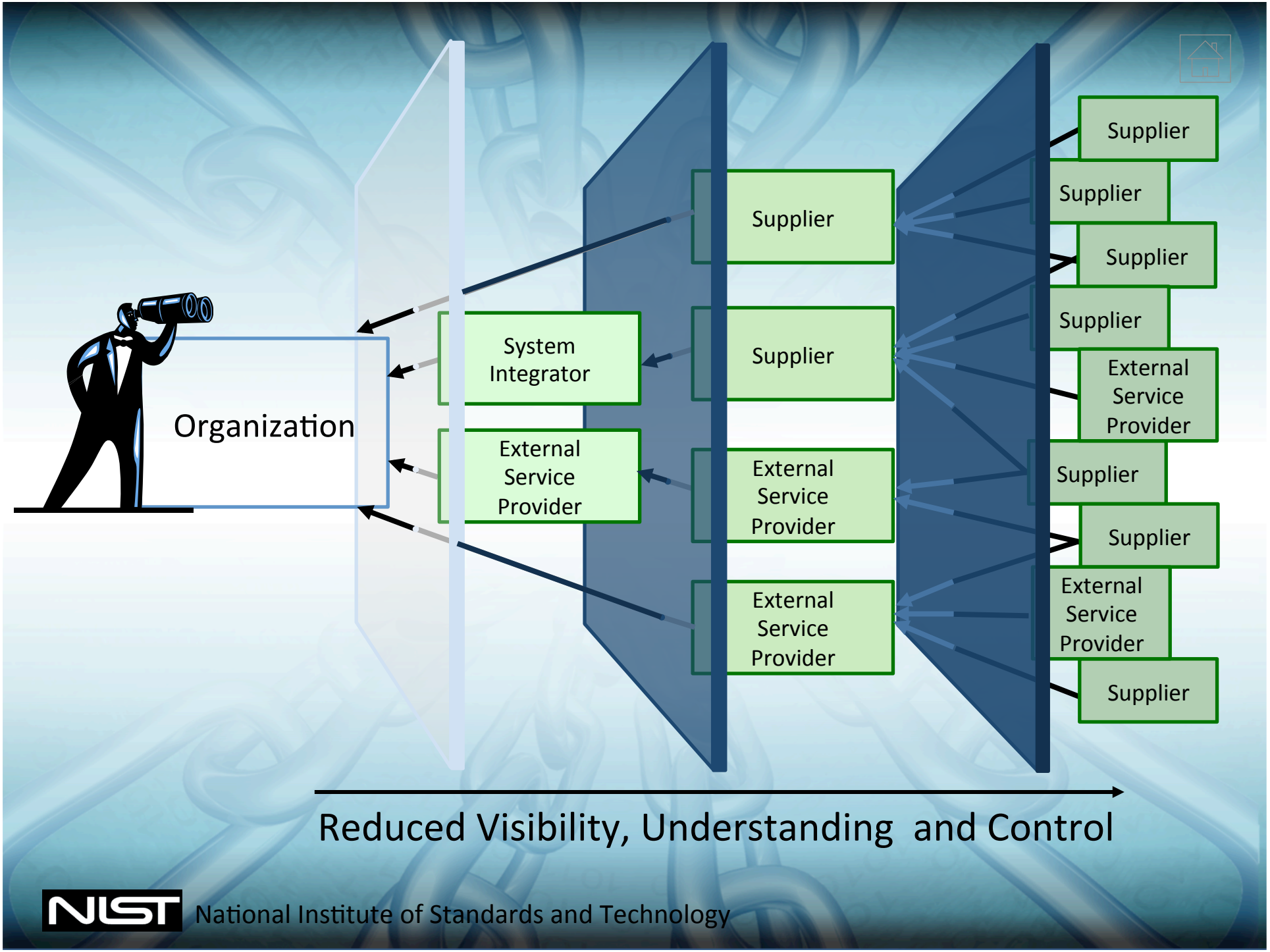
- Section 8(e) of the EO required GSA and DoD to:

  "*… make recommendations to the President, … on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration*"

- Report signed January 23, 2014 (http://gsa.gov/portal/content/176547)

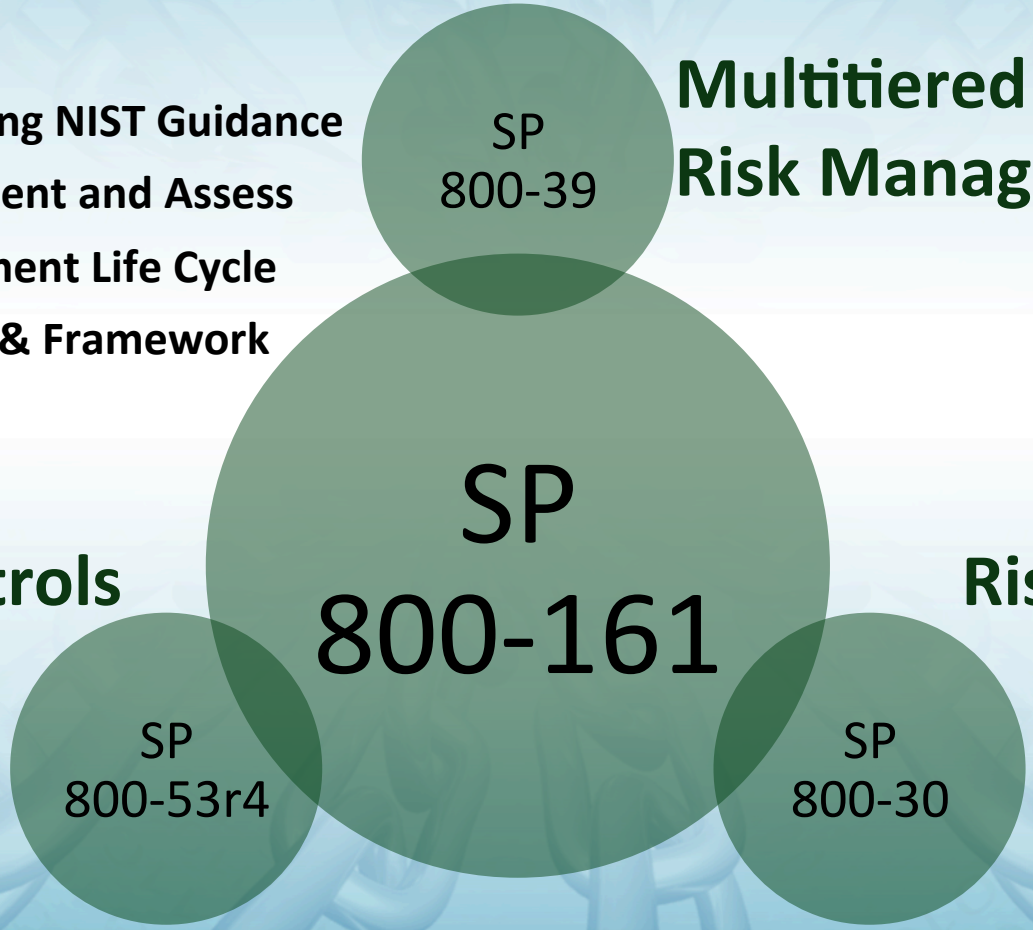


- Recommends six acquisition reforms:
  I. Institute Baseline Cybersecurity Requirements as a Condition of Contract Award for Appropriate Acquisitions
  II. Address Cybersecurity in Relevant Training
  III. Develop Common Cybersecurity Definitions for Federal Acquisitions
  IV. Institute a Federal Acquisition Cyber Risk Management Strategy
  V. Include a Requirement to Purchase from Original Equipment Manufacturers, Their Authorized Resellers, or Other "Trusted" Sources, Whenever Available, in Appropriate Acquisitions
  VI. Increase Government Accountability for Cyber Risk Management


Organization
System Integrator
External Service Provider
Supplier
Supplier
External Service Provider
External Service Provider
Supplier
Supplier
Supplier
External Service Provider
Supplier
Supplier
External Service Provider
Supplier
Reduced Visibility, Understanding and Control

SP 800-161, Supply Chain Risk Management for Federal Information Systems and Organizations

- **Building on existing NIST Guidance**
- **Ability to Implement and Assess**
- **System Development Life Cycle**
- **Threat Scenarios & Framework**
- **ICT SCRM Plan**



Multitiered Organizational Risk Management

Security Controls

Risk Assessment

Tiers


STRATEGIC (EXECUTIVE) RISK FOCUS
Communicating and sharing risk-related information from the strategic to tactical level, that is from the executives to the operators.
Communicating and sharing risk-related information from the tactical to strategic level, that is from the operators to the executives.
TIER 1
Organization
(Governance)
TIER 2
Mission / Business Process
(Information and Information Flows)
TIER 3
Information System
(Environment of Operation)
TACTICAL (OPERATIONAL) RISK FOCUS

DHS Sensitive Systems Policy Directive 4300A

DHS Sensitive Systems Policy Directive 4300A, Section 5.8 – Supply Chain
DHS depends on numerous supply chains for the hardware and software needed in order to effectively accomplish its missions. Many of these supply chains are independent of one-another and come with their own set of risks. **All programs need to make a risk management decision on how to best manage these risks. It is often no longer enough to perform "due diligence" at the beginning of an acquisition. Effective Supply Chain Risk Management (SCRM) requires the analysis of the Business Impact Assessment (BIA) to determine if the supply chain risks represent unacceptable business impact and what the best cost effective counter-measures are.** Because threats to that supply chain are continually evolving, including SCRM into the Continuous Monitoring process will be needed in the near future (e.g., continuous monitoring of integrators or logistics). **Some requirements may be included within DHS 4300A and the DHS Information Technology Acquisition Review (ITAR) process, which can respectively serve as policy and review mechanisms, but incorporation into the greater DHS acquisition process is vital for overall success.**

Policy ID	**DHS Policy Statements**	Use **Relevant Controls – NIST SP800-53r4 SA-12**
5.8.a	Business Impact Assessments (BIA) shall be used to determine the level of risk introduced to the system by the IT supply chain and whether the IT supply chain threat introduces sufficient risk to require the implementation of countermeasures.	
5.8.b	To protect against the supply chain threat, Components shall implement appropriate countermeasures, commensurate with the level of risk determined by the BIA.	

Additional Controls Relevant to ICT Services

NIST SP 800-161 Supply Chain Risk Management Practices

NIST SP 800-53 Revision 4 reflects evolving technology and threat space. Example areas include issues particular to mobile and cloud computing; insider threats; applications security; supply chain risks; advanced persistent threat; and trustworthiness, assurance, and resilience of information systems. The revision also contains a new appendix of privacy controls.

The Program Management (PM) family provides controls for information security programs themselves. It provides security controls at the organization level rather than the information system level.

New DHS Contract Clauses

HSAR Class Deviation 15-01 (March 2015)

Attachment 1: **Safeguarding of Sensitive Information**

Attachment 2: **Information Technology Security and Privacy Training**

Safeguarding of Sensitive Information

(a) *Applicability.* This clause applies to the Contractor, its subcontractors, and Contractor employees. The Contractor shall insert the substance of this clause in all subcontracts.

(b) *Definitions*. As used in this clause —

– Personally Identifiable Information (PII)

– Sensitive Information:

- Protected Critical Infrastructure Information (PCII)
- Sensitive Security Information (SSI)
- Information designated as “For Official Use Only”
- Information designated “sensitive” or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

"Personally Identifiable Information (PII)" means information that can be used to distinguish or trace an individual's identity. In performing this assessment, it is important for an agency to recognize that non-personally identifiable information can become personally identifiable information whenever additional information is made publicly available—in any medium and from any source—that, combined with other available information, could be used to identify an individual.

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee)

Safeguarding of Sensitive Information

(c) *Authorities.* The Contractor shall follow all current versions of Government policies and guidance accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors, or available upon request from the Contracting Officer, including but not limited to:

(1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information

(2) DHS Sensitive Systems Policy Directive 4300A

(3) DHS 4300A Sensitive Systems Handbook and Attachments

(4) DHS Security Authorization Process Guide

(5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information

Safeguarding of Sensitive Information

(6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program

(7) DHS Information Security Performance Plan (current FY)

(8) DHS Privacy Incident Handling Guidance

(9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at http://csrc.nist.gov/groups/STM/cmvp/standards.html

(10) NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at http://csrc.nist.gov/publications/PubsSPs.html

(11) NIST SP 800-88 Guidelines for Media Sanitization accessible at http://csrc.nist.gov/publications/PubsSPs.html

Safeguarding of Sensitive Information

(d) *Handling of Sensitive Information.* Contractor compliance with this clause, as well as the policies and procedures described below, is required.

(1) DHS policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. *MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information* describes how Contractors must handle sensitive but unclassified information.

(2) The Contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the Contractor except as specified in the contract.

Safeguarding of Sensitive Information

(3) **All Contractor employees with access to sensitive information shall execute *DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA),* as a condition of access to such information**. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer's Representative (COR) no later than two (2) days after execution of the form.

(4) The Contractor's **invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII.** It is acceptable to maintain in these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.

Safeguarding of Sensitive Information

(e) *Authority to Operate*. The Contractor shall not input, store, process, output, and/or transmit sensitive information within a Contractor IT system without an Authority to Operate (ATO) signed by the Headquarters or Component CIO, or designee, in consultation with the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. The Contractor shall adhere to current Government policies, procedures, and guidance for Security Authorization (SA) process as defined below.

(1) Complete the Security Authorization process. The SA process shall proceed according to the *DHS Sensitive Systems Policy Directive 4300A* (Version 11.0, April 30, 2014), or any successor publication, *DHS 4300A Sensitive Systems Handbook* (Version 9.1, July 24, 2012), or any successor publication, and the *Security Authorization Process Guide* including templates.

(i) Security Authorization Process Documentation

(ii) Independent Assessment.

(iii) Support the completion of the Privacy Threshold Analysis (PTA)

Safeguarding of Sensitive Information

(i) Security Authorization Process Documentation. SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates.

SA documentation consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s).

During the development of SA documentation, the Contractor shall submit a signed SA package, validated by an independent third party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the IT system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. The Government's acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the IT system controls are implemented and operating effectively..

Safeguarding of Sensitive Information

(ii) Independent Assessment. Contractors shall have an independent third party validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in *NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations*. The Contractor shall address all deficiencies before submitting the SA package to the Government for acceptance.

Safeguarding of Sensitive Information

(iii) Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the SA process, the Contractor may be required to support the Government in completion of the PTA.

- **The requirement to complete a PTA is triggered by creation, use, modification, upgrade, or disposition of a Contractor IT system that will store, maintain and use PII, and must be renewed at least every 3 years.**
- Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required.
- The Contractor shall provide all support necessary to assist the Department in completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones.
- Support in this context includes responding timely to requests for information from the Government about the use, access, storage, and maintenance of PII on the Contractor's system, and providing timely review of relevant compliance documents for factual accuracy.
- **Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at http://www.dhs.gov/privacy-compliance**

Safeguarding of Sensitive Information

(2) *Renewal of ATO.* Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods:

- Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or
- Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90 day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules.

The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

Safeguarding of Sensitive Information

(3) *Security Review.* The Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, the Office of the Inspector General, and other Government organizations access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract.

- The Contractor shall, through the Contracting Officer and COR, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to the DHS.
- Access shall be provided, to the extent necessary as determined by the Government, for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of Government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

Safeguarding of Sensitive Information

(4) *Continuous Monitoring.* All Contractor-operated systems that input, store, process, output, and/or transmit sensitive information shall meet or exceed the continuous monitoring requirements identified in the *Fiscal Year 2014 DHS Information Security Performance Plan,* or successor publication.

- The plan is updated on an annual basis.
- The Contractor shall also store monthly continuous monitoring data at its location for a period not less than one year from the date the data is created.
- The data shall be encrypted in accordance with *FIPS 140-2 Security Requirements for Cryptographic Modules* and shall not be stored on systems that are shared with other commercial or Government entities.
- The Government may elect to perform continuous monitoring and IT security scanning of Contractor systems from Government tools and infrastructure.

Safeguarding of Sensitive Information

(5) *Revocation of ATO.* In the event of a sensitive information incident, the Government may suspend or revoke an existing ATO (either in part or in whole).

- If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct the Contractor to take additional security measures to secure sensitive information.
- These measures may include restricting access to sensitive information on the Contractor IT system under this contract.
- Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

Safeguarding of Sensitive Information

(6) *Federal Reporting Requirements.* Contractors operating information systems on behalf of the Government or operating systems containing sensitive information shall comply with Federal reporting requirements. Annual and quarterly data collection will be coordinated by the Government.

- Contractors shall provide the COR with requested information within three (3) business days of receipt of the request. Reporting requirements are determined by the Government and are defined in the *Fiscal Year 2014 DHS Information Security Performance Plan,* or successor publication.
- The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for Contractor systems.

Safeguarding of Sensitive Information

(f) *Sensitive Information Incident Reporting Requirements.*

(1) All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of discovery in accordance with *4300A Sensitive Systems Handbook Incident Response and Reporting* requirements.

- When notifying the Headquarters or Component SOC, the Contractor shall notify the Contracting Officer, COR, Headquarters or Component Privacy Officer, and US-CERT using contact information identified in the contract.
- If the incident is reported by phone or the Contracting Officer's email address is not immediately available, the Contractor shall contact the Contracting Officer immediately after reporting the incident to the Headquarters or Component SOC. The Contractor shall not include any sensitive information in the subject or body of any e-mail.

Safeguarding of Sensitive Information

- To transmit sensitive information, the Contractor shall use *FIPS 140-2 Security Requirements for Cryptographic Modules* compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment.
- A sensitive information incident shall not, by itself, be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for sensitive information, or has otherwise failed to meet the requirements of the contract.

Safeguarding of Sensitive Information

(2) If a sensitive information incident involves PII or SPII, in addition to the reporting requirements in *4300A Sensitive Systems Handbook Incident Response and Reporting*, Contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

- Data Universal Numbering System (DUNS);
- Contract numbers affected unless all contracts by the company are affected;
- Facility CAGE code if the location of the event is different than the prime contractor location;
- Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
- Contracting Officer POC (address, telephone, email); Contract clearance level;
- Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
- Government programs, platforms or systems involved; Location(s) of incident;
- Date and time the incident was discovered;
- Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
- Description of the Government PII and/or SPII contained within the system;
- Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and any additional information relevant to the incident.

Safeguarding of Sensitive Information

(g) *Sensitive Information Incident Response Requirements.*

- All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer in consultation with the Headquarters or Component CIO and Headquarters or Component Privacy Officer.

- The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.

Safeguarding of Sensitive Information

(3) Incident response activities determined to be required by the Government may include, but are not limited to, the following:

- Inspections,
- Investigations,
- Forensic reviews, and
- Data analyses and processing.

(4) The Government, at its sole discretion, may obtain the assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

Safeguarding of Sensitive Information

(h) *Additional PII and/or SPII Notification Requirements*.

(1) The Contractor shall have in place procedures and the capability to notify any individual whose PII resided in the Contractor IT system at the time of the sensitive information incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the Contracting Officer.

- The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, utilizing the *DHS Privacy Incident Handling Guidance*.
- The Contractor shall not proceed with notification unless the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.

Safeguarding of Sensitive Information

(2) Subject to Government analysis of the incident and the terms of its instructions to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government.

Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:

- A brief description of the incident;
- A description of the types of PII and SPII involved;
- A statement as to whether PII or SPII was encrypted or protected by other means;
- Steps individuals may take to protect themselves;
- What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and
- Information identifying who individuals may contact for additional information.

Safeguarding of Sensitive Information

(i) ***Credit Monitoring Requirements*****.** In the event that a sensitive information incident involves PII or SPII, the Contractor may be required to, as directed by the Contracting Officer:

- Provide notification to affected individuals as described above; and/or
- Provide credit monitoring services to individuals whose data was under the control of the Contractor or resided in the Contractor IT system at the time of the sensitive information incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the Contractor has no affiliation.
- Establish a dedicated call center.

(j) ***Certification of Sanitization of Government and Government-Activity-Related Files and Information.*** As part of contract closeout, the Contractor shall submit the certification to the COR and the Contracting Officer following the template provided in *NIST Special Publication 800-88 Guidelines for Media Sanitization*.

Info Tech Security and Privacy Training

INFORMATION TECHNOLOGY SECURITY AND PRIVACY TRAINING (MAR 2015) -- Requirements

(a) ***Applicability.*** This clause applies to the Contractor, its subcontractors, and Contractor employees. The Contractor shall insert the substance of this clause in all subcontracts.

(b) ***Security Training Requirements*****.**

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change.

Info Tech Security and Privacy Training

- The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract.
- Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year.
- Any new Contractor employees assigned to the contract shall complete training before accessing sensitive information under contract. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors.
- The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer's Representative (COR) not later than 30 days after contract award.
- Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

Info Tech Security and Privacy Training

(2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information.

- The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information.
- The DHS Rules of Behavior is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually and the COR will provide notification when a review is required.

Info Tech Security and Privacy Training

(c) *Privacy Training Requirements.* All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take *Privacy at DHS: Protecting Personal Information* before accessing PII and/or SPII.

- The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall also complete the training before accessing PII and/or SPII.
- The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the COR not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

Software & Supply Chain Assurance:

Enabling Enterprise Resilience through Software Assurance and Supply Chain Risk Management

Homeland Security

Joe Jarzombek, PMP, CSSLP
Director for Software & Supply Chain Assurance
Stakeholder Engagement & Cyber Infrastructure Resilience
Cyber Security & Communications
joe.jarzombek@hq.dhs.gov